Single Connect™

Privileged Access Management

2019

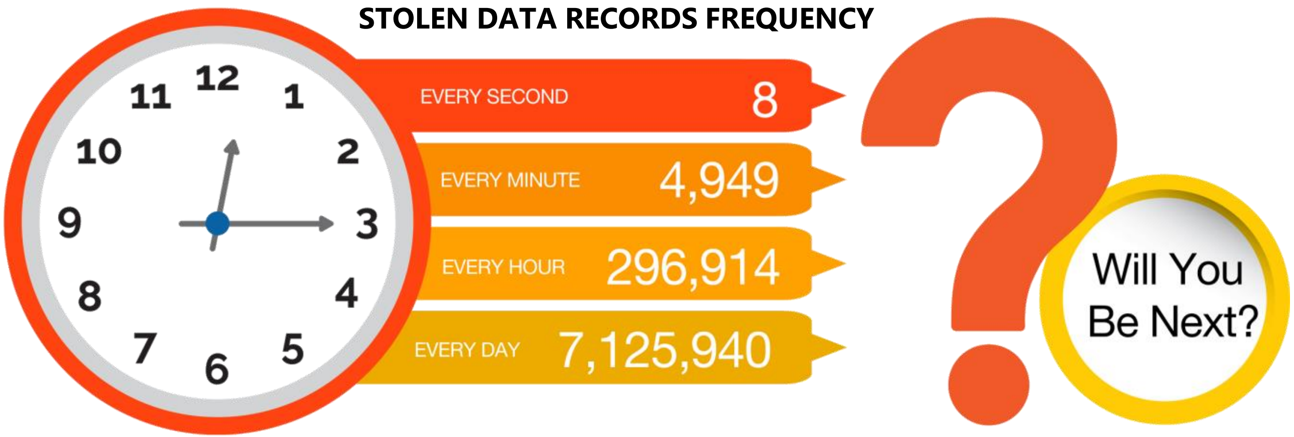
Company Overview

Protect What You Connect™

Single Connect™ enables IT managers and network admins to efficiently secure the access, control configurations and indisputably record all activities in the data center or network infrastructure, in which any breach in privileged accounts access might have material impact on business continuity.

Krontech is headquartered in New Jersey with research and development facilities in Istanbul, and regional sales and support offices in LATAM, CIS, Middle East and Africa and Asia Pacific.

The Privileged Access Problem



2.6 billion

records breached in 2017

81% of

breaches due to stolen passwords

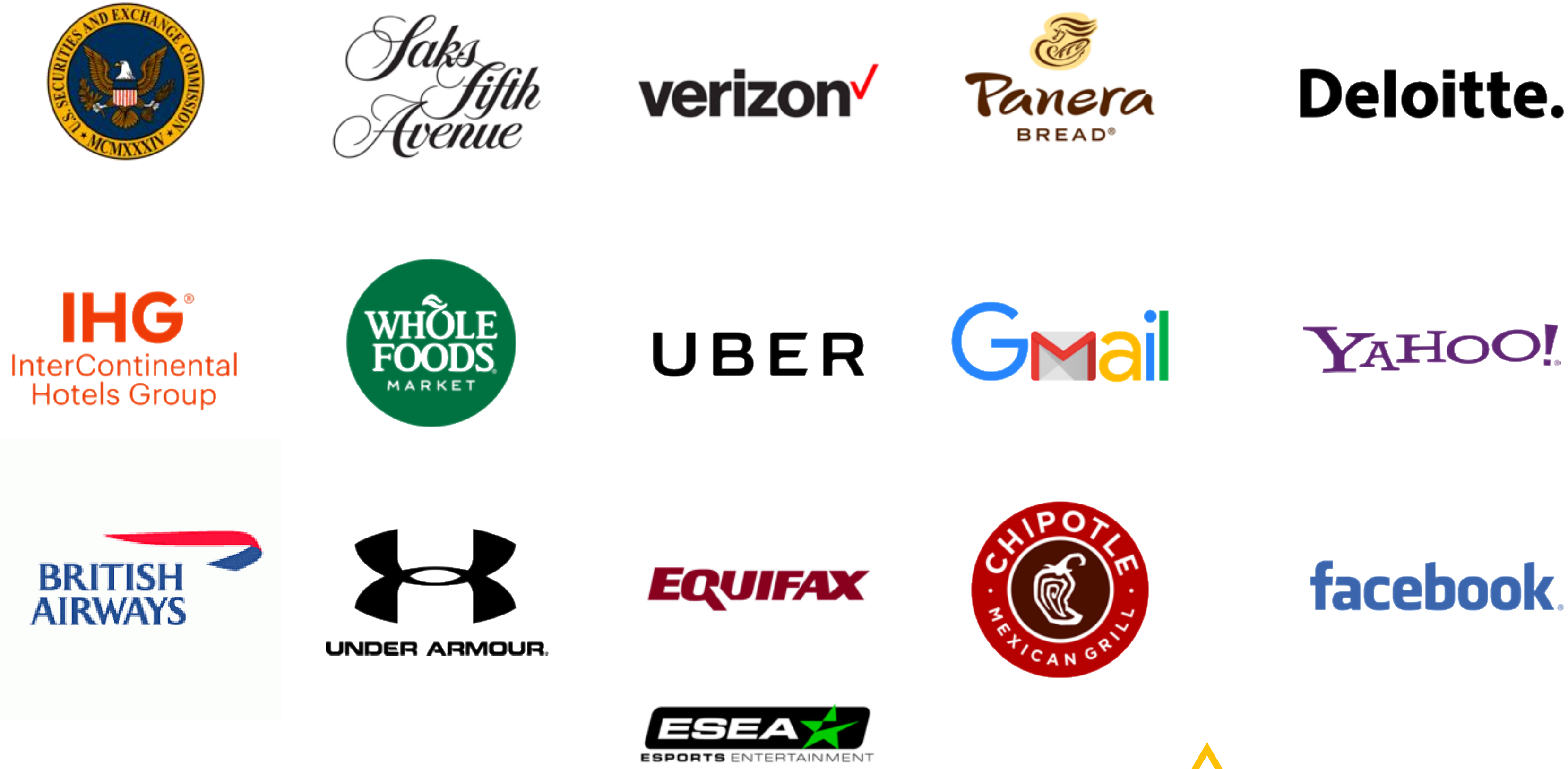
43% of

the successful breaches were linked to internal actors

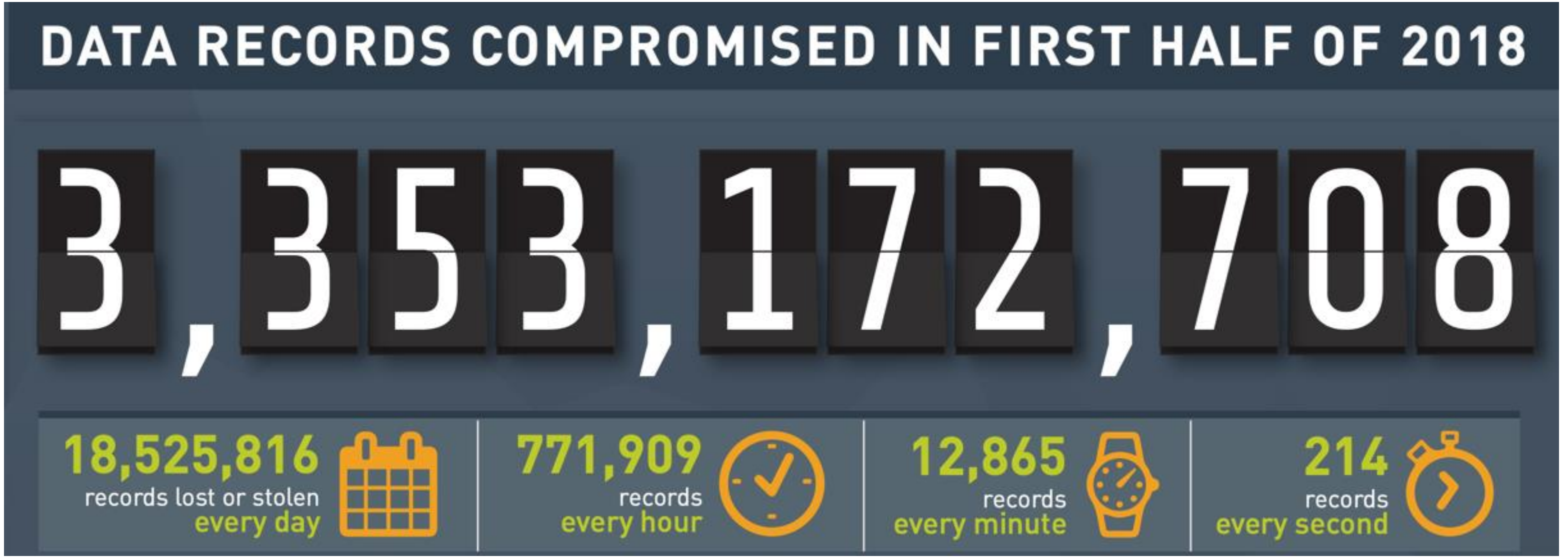
$3.86 M

Average cost of a data breach

Breached Companies



Data records lost or stolen btw. Jan-Jun 2018



DATA RECORDS COMPROMISED IN FIRST HALF OF 2018

3,353,172,708

18,525,816 records lost or stolen every day

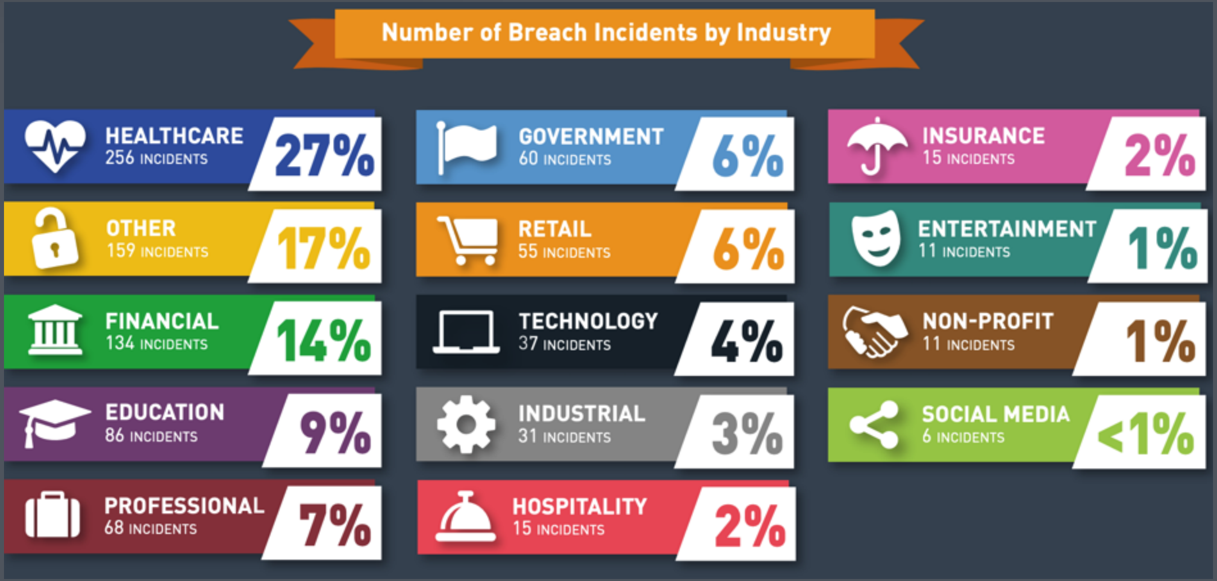
771,909 records every hour

12,865 records every minute

214 records every second

https://breachlevelindex.com/

Data Breach Incidents by Industry Jan-Jul 2018

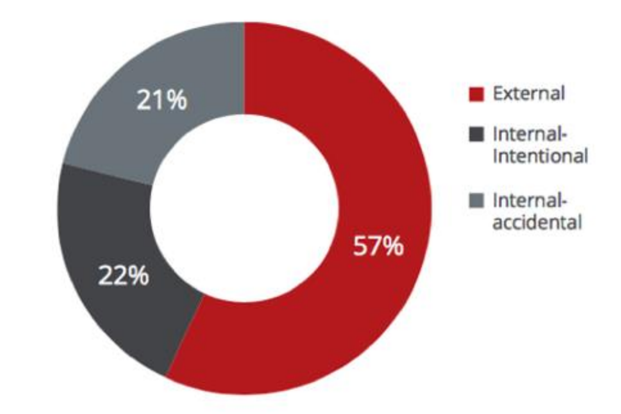


Number of Breach Incidents by Industry

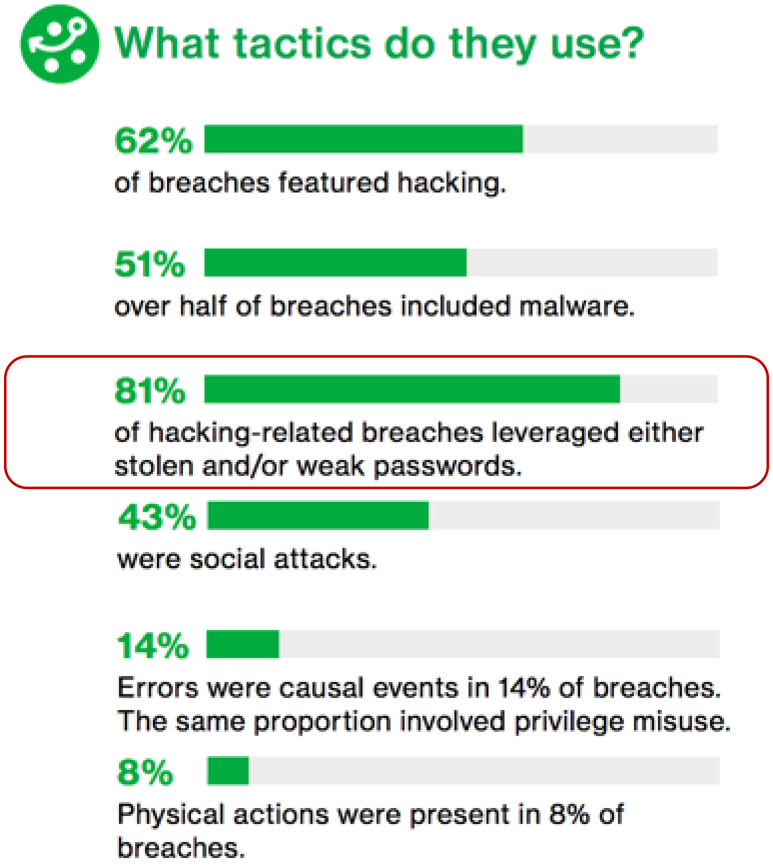
HEALTHCARE	256 INCIDENTS	27%
OTHER	159 INCIDENTS	17%
FINANCIAL	134 INCIDENTS	14%
EDUCATION	86 INCIDENTS	9%
PROFESSIONAL	68 INCIDENTS	7%
GOVERNMENT	60 INCIDENTS	6%
RETAIL	55 INCIDENTS	6%
TECHNOLOGY	37 INCIDENTS	4%
INDUSTRIAL	31 INCIDENTS	3%
HOSPITALITY	15 INCIDENTS	2%
INSURANCE	15 INCIDENTS	2%
ENTERTAINMENT	11 INCIDENTS	1%
NON-PROFIT	11 INCIDENTS	1%
SOCIAL MEDIA	6 INCIDENTS	<1%

GEMALTO

Data Breaches



Actors Involved in Data Breaches
McAfee, Grand Theft Data



What tactics do they use?

62%
of breaches featured hacking.

51%
over half of breaches included malware.

81%
of hacking-related breaches leveraged either stolen and/or weak passwords.

43%
were social attacks.

14%
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%
Physical actions were present in 8% of breaches.

Verizon 2017 Data Breach Investigations Report

Privileged Accounts

The Five “W”s of Privileged Access

Who	When	What	Where	Why
Administrators (System, DB and APP)	Continuous	Broad	Broad	Flexible
Operators, Help Desk	Continuous	Medium	Broad	Flexible
Developers	Continuous	Restricted	Restricted	Flexible, r/o
Project Staff	Occasional	Limited	Narrow	Limited
Third Parties (Contractors, Vendors)	One-Off	Depends	Narrow	Limited

GARTNER

Privileged Accounts

Best Practices

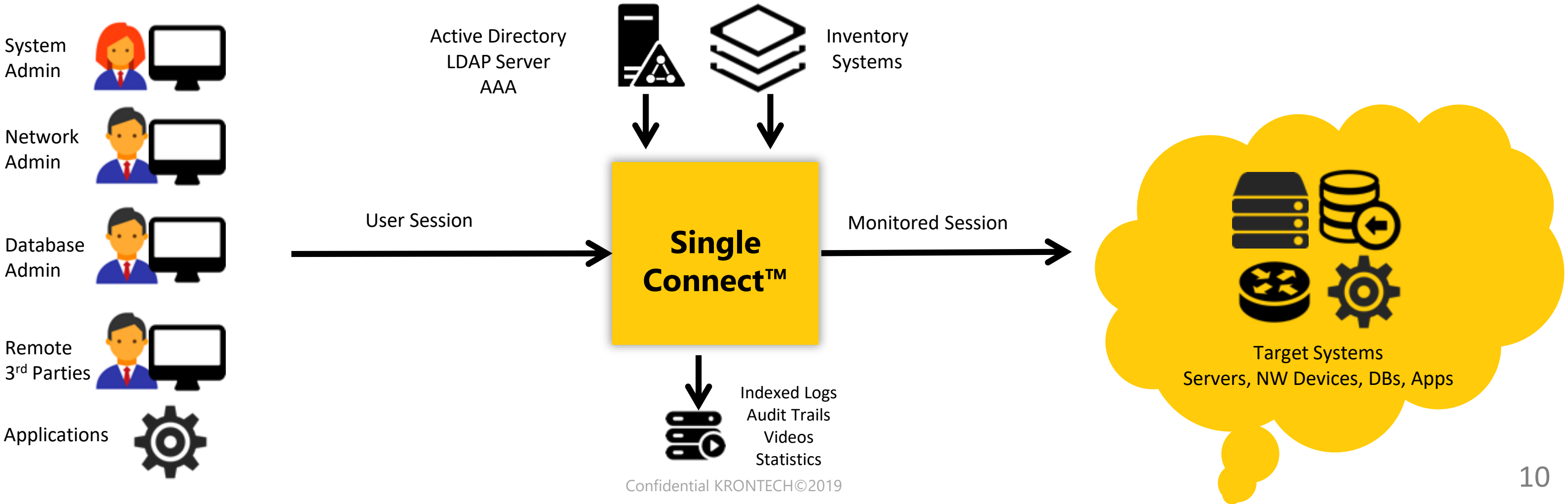
- Implement strict password and account management policies
- Enforce separation of duties and least privilege
- Log and record all actions of administrators and 3rd party users
- Use layered defense against remote attacks
- Deactivate access following termination
- Collect and save data for use in investigations

Single Connect™

Single Connect™ is a comprehensive Privileged Access Management (PAM) software suite designed to prevent internal and external attacks aiming to compromise privileged accounts

Complete set of tools and features to help secure the access, control configurations, monitor in real-time and indisputably record all activities in a datacenter or network infrastructure

Providing critical tools, monitoring and reporting for internal audit and regulatory compliance (including GDPR, PCI DSS, SWIFT, HIPAA, ISO 27002)



Single Connect Modules

Single Connect Modules

Dynamic Password Controller

Takes control of device and database passwords, providing security while sustaining efficiency.

Session Manager

Logging and recording of all sessions, including command and context-aware filtering.

MFA Manager

Additional layers of authentication integrating mobile device, geo-location, and time.

TACACS+ Access Manager

Protocol-based security software unifies AAA, Active Directory, LDAP, & TACACS+.

Data Access Manager

Securing Data Access with logging, policy enforcement, and real time data masking.

Cloud PAM

PAM services from the cloud; secures 3rd party remote access from the cloud.

Privileged Task Automation Manager

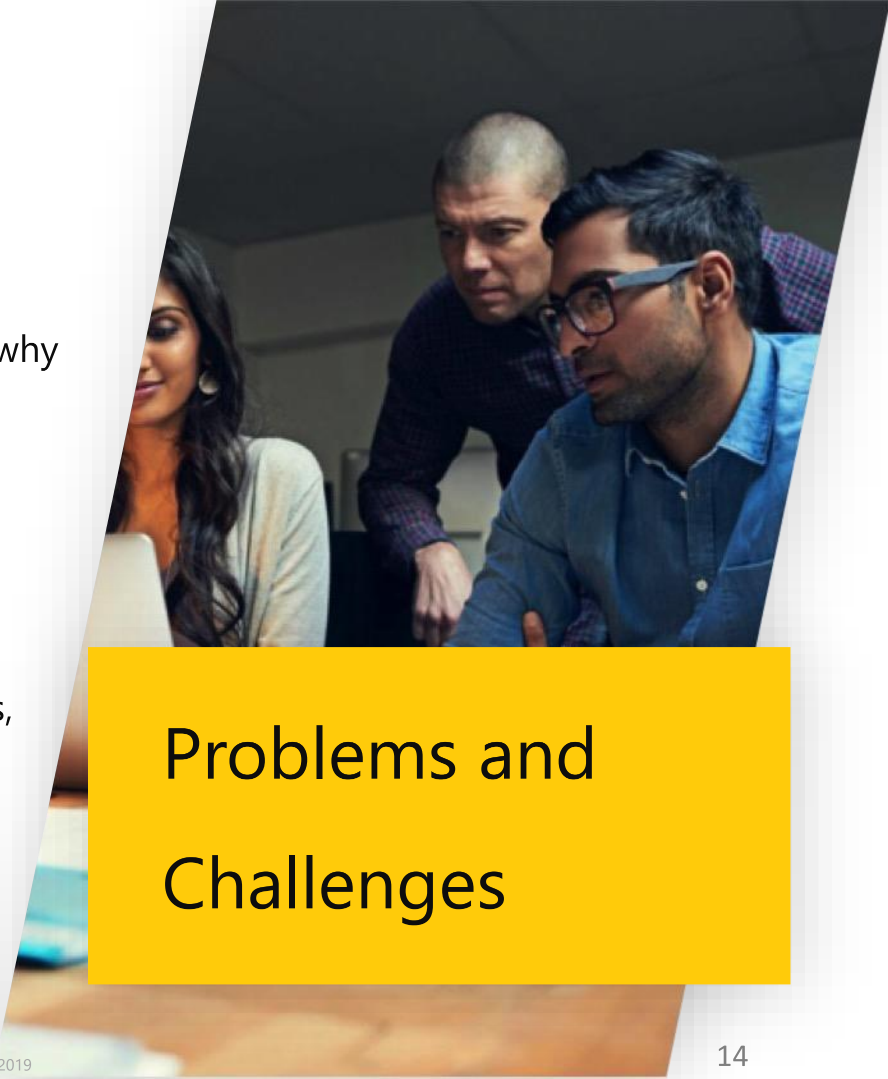
Privileged task and configuration to improve efficiency and security

Dynamic Password Controller

Eliminates account theft risks by managing system and admin passwords centrally

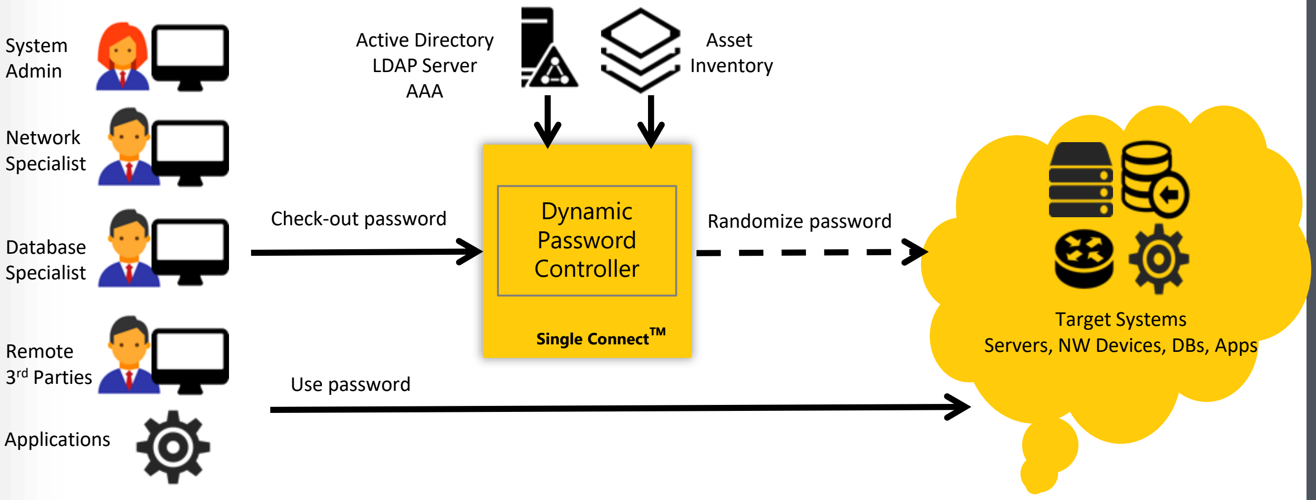
Dynamic Password Controller

- Easy to remember passwords
- Keeping track of passwords, who used, when and why
- Using same password for many systems
- Not changing passwords at regular intervals
- No or minimal accountability
- Applications store credentials in configuration files, DB's or source codes
- Password sharing among colleagues



Problems and Challenges

Dynamic Password Controller Overview



Dynamic Password Controller is a password vault which stores and rotates privileged (admin, system, root, etc.) accounts centrally and securely.

Users log-in to Single Connect with their personal accounts, check-out the credentials of a privileged account and then uses the password to connect to target endpoints.

Searchable log records and audit trails are generated to meet the security and compliance requirements.

- **Operating Systems**

  Windows/Linux/Unix

- **Database Systems**

  Oracle, MySQL, MSSQL, PostgreSQL, etc.

- **Network Devices and Appliances**

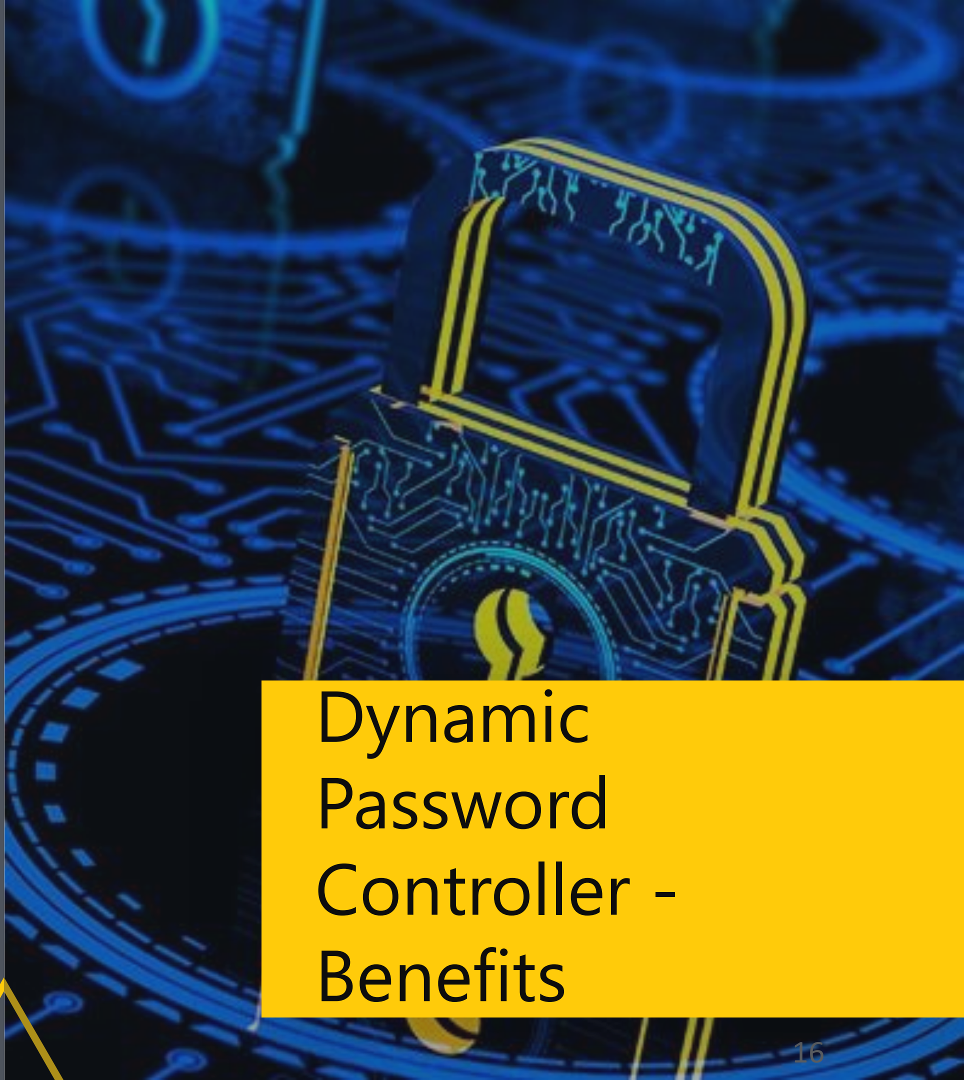
  With CLI interfaces

- **Applications**

  With password change API

Dynamic Password Controller - Benefits

- Prevent unauthorized access to critical systems
- Stop attacks using stolen privileged credentials
- Password usage history of which individual users accessed to what, when and why
- Enforce role-based access controls
- Change passwords after each usage and at regular intervals to ensure maximum strength
- Eliminate password sharing among employees
- Auto-lock user account on employee termination
- Eliminate embedded passwords that are stored in unencrypted text files, DB's or source codes

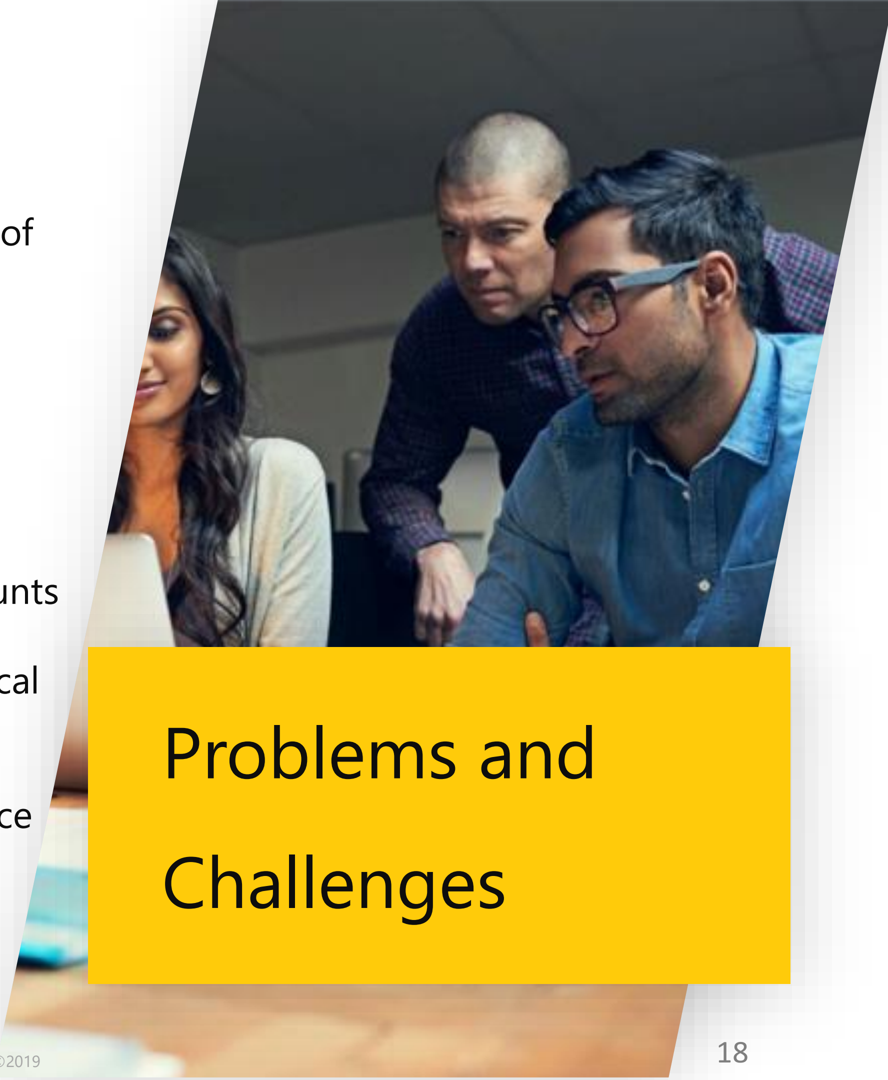


Session Manager

Monitor and control all privileged sessions on critical systems

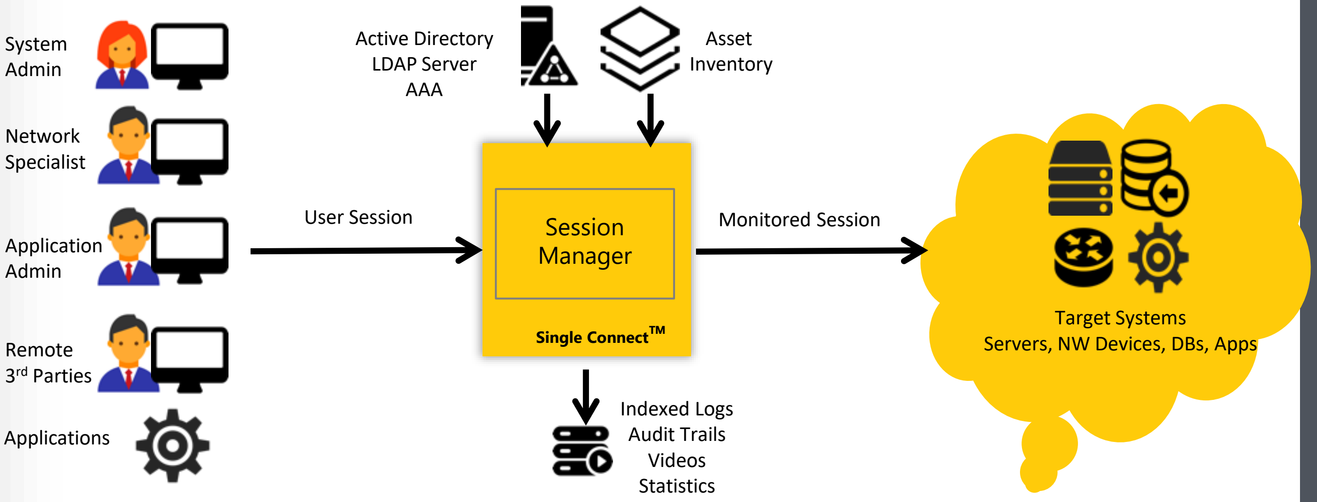
Session Manager

- Complexity of access management for hundreds of users connecting to thousands of systems
- Lack of central access control point for critical systems
- Granting users more privileges than they need
- No or minimal accountability for privileged accounts
- Lateral movement and spread of malware to critical systems
- Lack of data and reports for regulatory compliance and audits
- Unsecure 3rd party remote access



Problems and Challenges

Session Manager Overview



Single Connect Session Manager secures access, controls configuration changes, and records all privileged activities in a datacenter or network infrastructure.

Session Manager isolates critical target systems from users. Agentless, man-in-the-middle approach of Session Manager eliminates the need of software agents to be deployed on target systems or user computers.

Provides role-based segregation of duties and least privilege.

Supports virtually all types of sessions :

Console Sessions

SSH, TELNET

Remote Desktop Sessions

RDP, VNC

Web Sessions

HTTP/S

Applications

Cloud, on-prem or custom applications

Session Manager Benefits

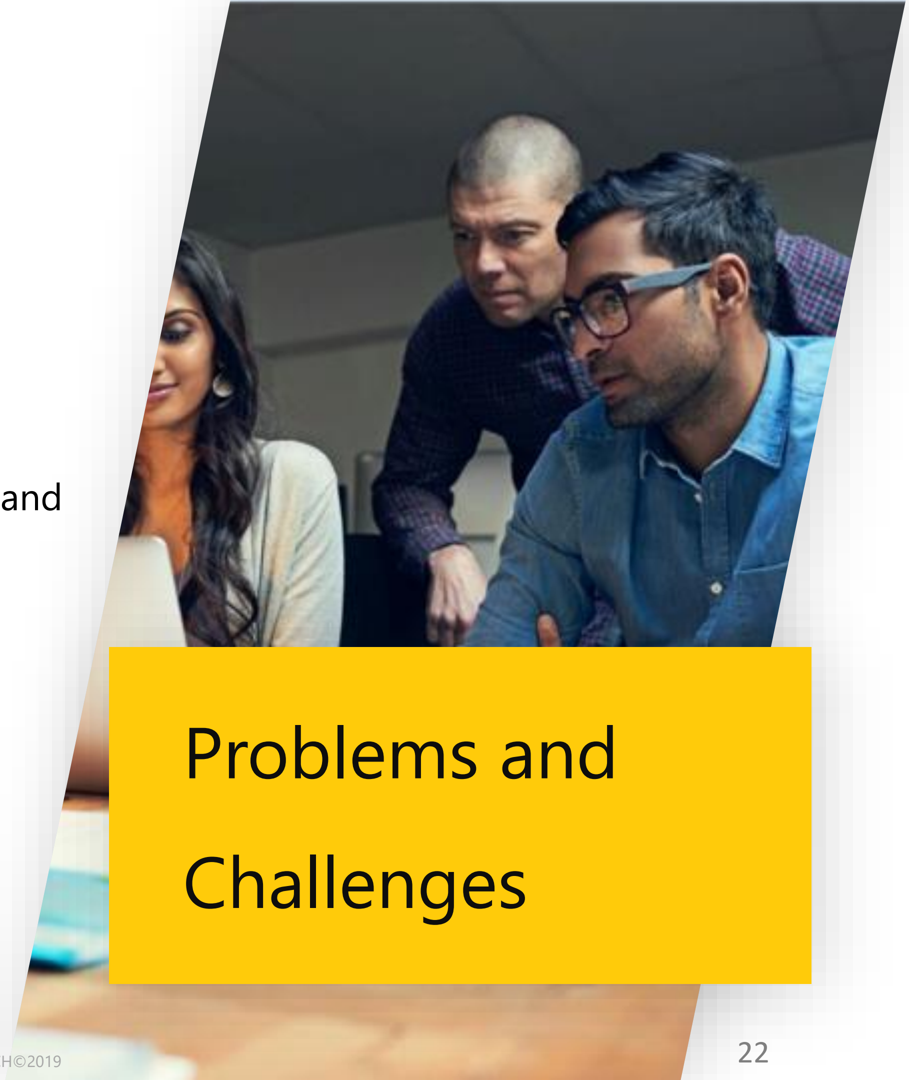
- Unified visibility with searchable command / keystroke logs and replayable video recordings
- Isolation of critical target systems from user network
- Provides least privilege functions including command or application-based restrictions, managerial approval, geo-location confirmation, time & date based access
- Detects and stops malicious activities before they occur
- Enforces role based security policies centrally and silently
- Users continue to use their own native client apps seamlessly
- Addresses regulatory requirements for privileged sessions
- Fastest to deploy PAM solution with scalable and pre-integrated modular architecture.

MFA Manager

Additional layer of authentication using mobile phone and geo-location

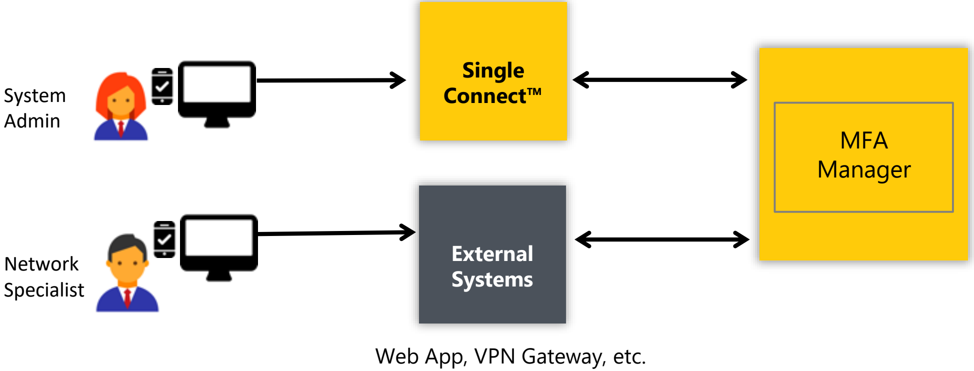
MFA Manager

- Account thefts via phishing, malwares, etc.
- Easy to discover user credentials
- Need for extra precautions for 3rd party access and remote connections
- Securing external application connections



Problems and Challenges

MFA Manager Overview

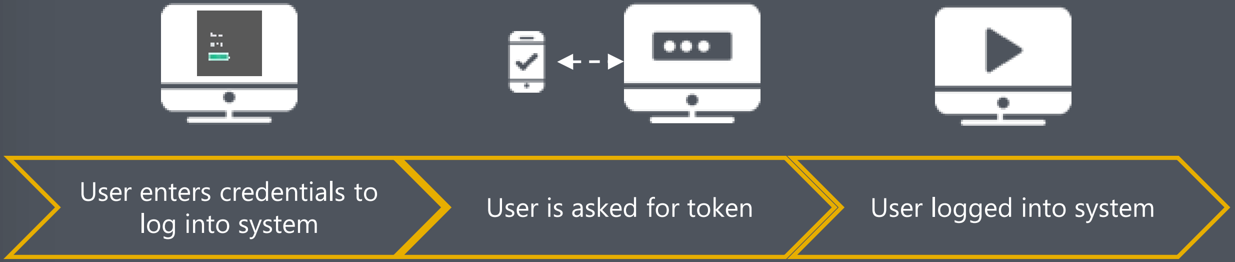


Additional layer of security on top of user credentials for authentication.

MFA Manager ensures that users are who they claim to be.

You are secure even if username/password of your internal privileged account is hacked.

MFA Manager is pre-integrated with Single Connect modules, and ready to integrate with external systems.



Online Token
SMS, Email, Mobile App

Offline Token
Mobile App, Hard Token

Advanced Controls
Geo-Fencing and Time Restrictions

Standards-based Integration
RADIUS and REST API interfaces

MFA Benefits

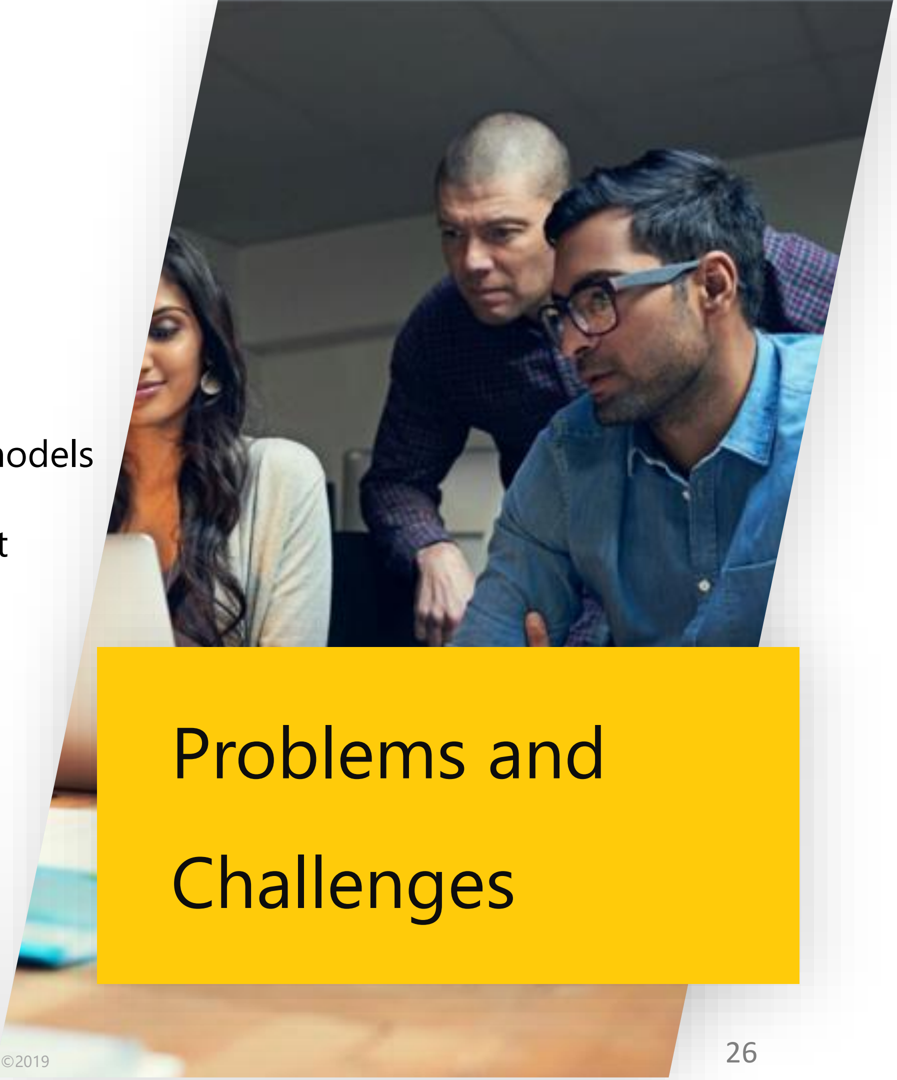
- Prevents unauthorized access even the user account is stolen
- Strengthens the logon process even the password is weak or non-changed, by providing One-Time tokens
- Eliminates the risks of password sharing among colleagues
- Enables geo-location and time restrictions for secure access
- Enables multi-factor authentication for external apps
- Pre-integrated with Single Connect modules

TACACS+ Access Manager

Protocol-based security software that unifies AAA, Active Directory, LDAP, & TACACS+

TACACS+ Access Manager

- Thousands of legacy network elements to be managed with TACACS and RADIUS protocols
- Complexity of legacy TACACS policy definition models
- Several TACACS and RADIUS servers for different departments within the same enterprise
- End-of-life status of Cisco ACS

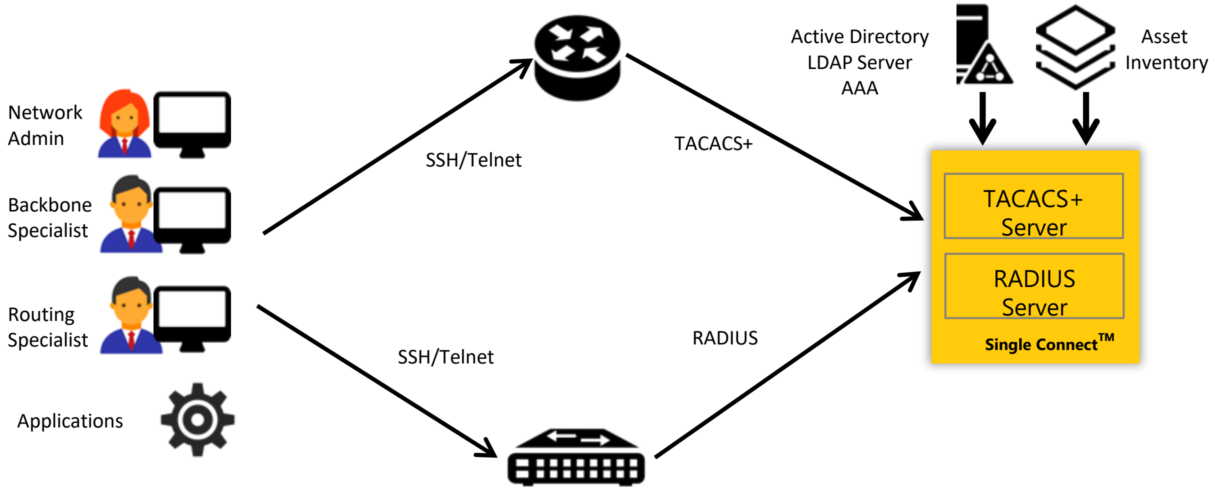


Problems and Challenges

TACACS+ Access Manager

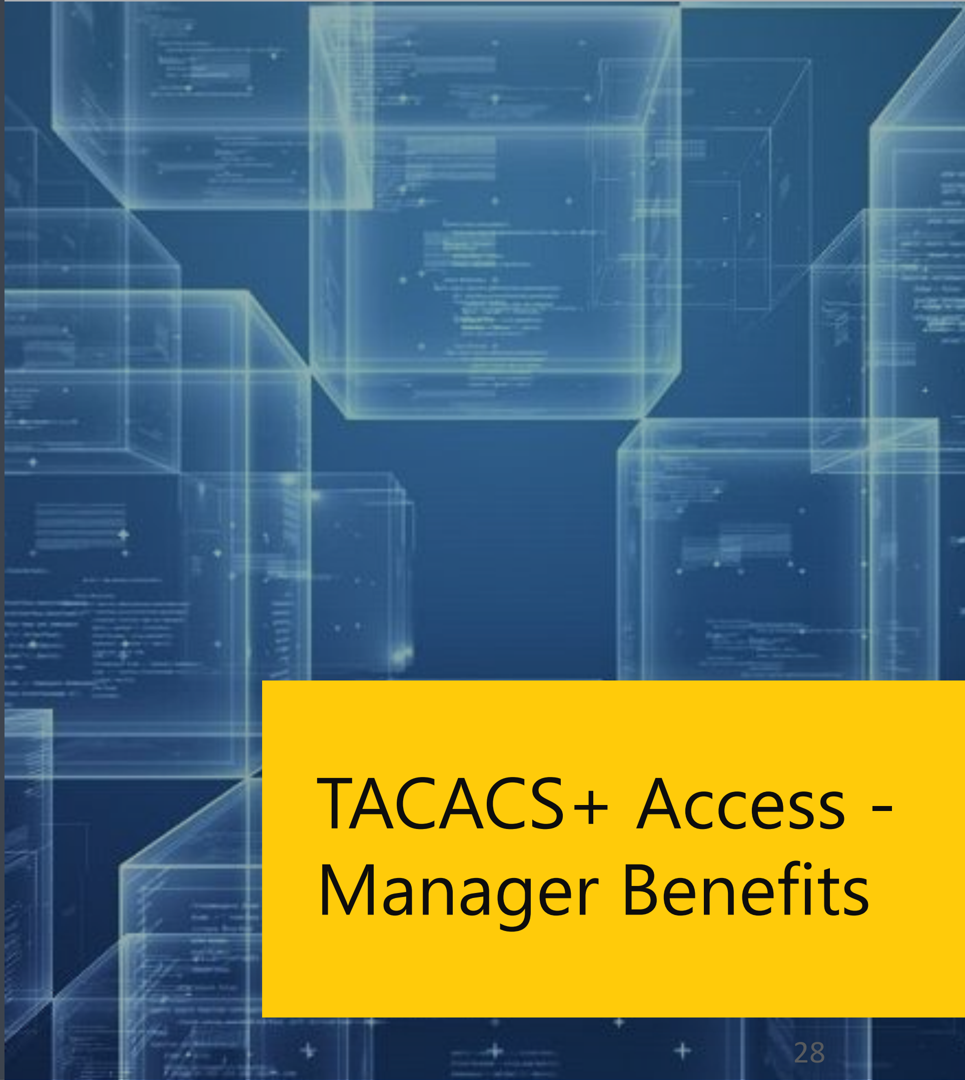
TACACS+ (Terminal Access Controller Access-Control System) and RADIUS (Remote Access Dial-In User Service) are used to control access to network devices via SSH/TELNET sessions.

Single Connect has built-in and pre-integrated TACACS+ and RADIUS servers that provide AAA (Authentication, Authorization and Accounting) services for network infrastructure.



TACACS+ Access - Manager Benefits

- Standalone AAA server solution for RADIUS and TACACS+ protocols
- Provides least privilege functions including command-based restrictions, and privilege levels
- Enforces security policies centrally and silently to direct connections to network elements
- Supports configuration of custom AVP (Attribute Value Pair) definitions
- Highest performance and scalability in the market supporting up to 250,000 devices with a single box

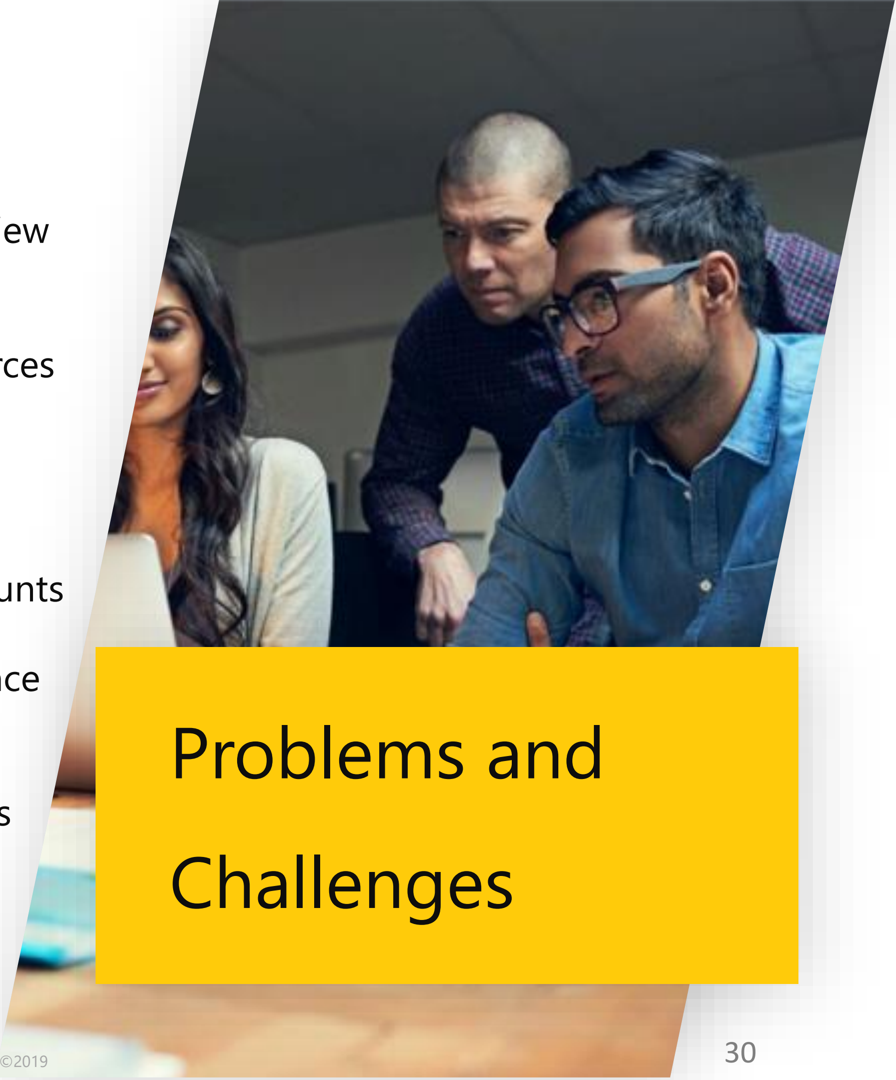


Data Access Manager

Securing Data Access with logging, policy enforcement, and real time data masking

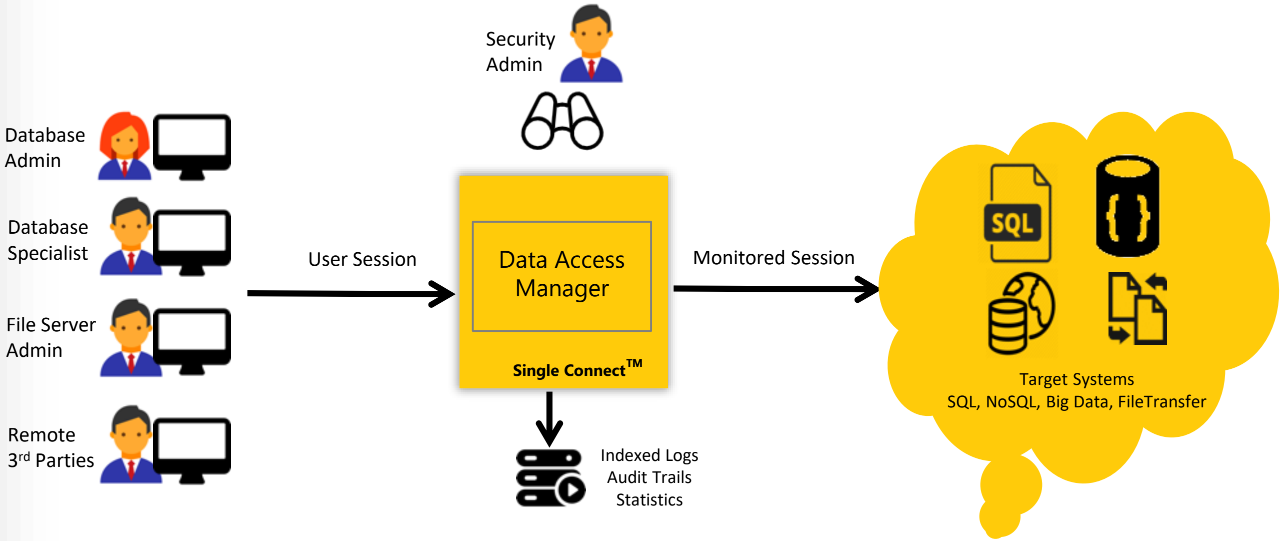
Data Access Manager

- Highly privileged Database Administrators can view or change any piece of sensitive data
- Lack of central access control point for data sources
- Tradeoff between the level of security and performance of databases
- No or minimal accountability for DB admin accounts
- Lack of data and reports for regulatory compliance and audits
- Unsecure 3rd party remote access to data sources



Problems and Challenges

Data Access Manager Overview



Single Connect Data Access Manager isolates sessions of privileged users (such as DB admins) and secures access, controls changes, and logs all activities of such users on sensitive data sources such as databases and files transfer servers.

Agentless, man-in-the-middle approach of Session Manager eliminates the need of software agents to be deployed on target systems or user computers.

Provides role-based segregation of duties and least privilege.

Supports wide range of Data Sources

- Oracle
- MSSQL
- MySQL
- Teradata
- Cassandra
- Hive

Data Access Manager – Dynamic Data Masking

Data masking is a technology aimed at preventing the abuse of sensitive/confidential data by giving users masked or fictitious (yet realistic) data instead of real sensitive data

Dynamic Data Masking is necessary if users or applications need to access production data that require masked or representative but still coherent data without changing the source data

ORIGINAL DATA

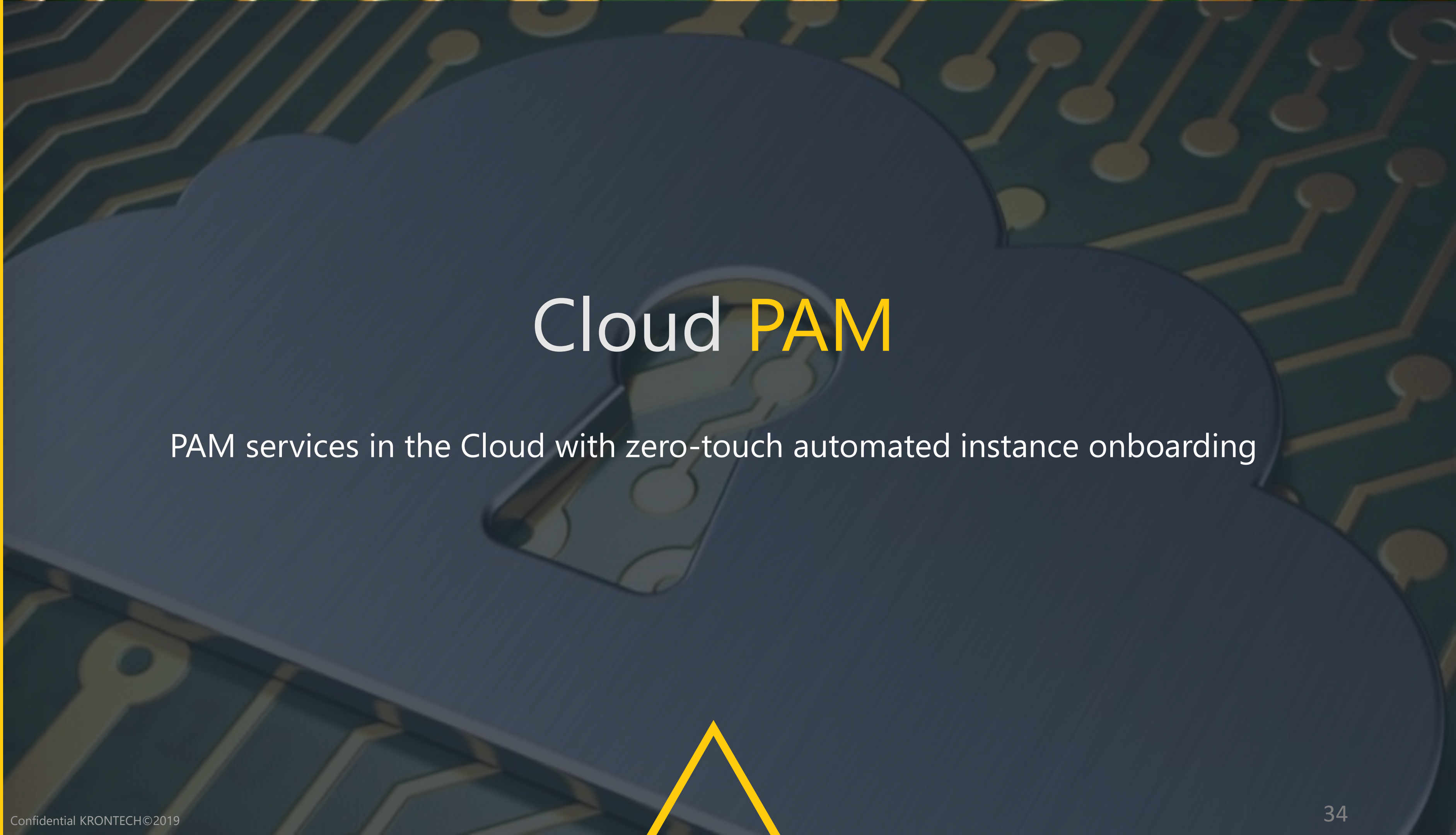
Name	Phone	Birth Date
John Doe	511-336-44-55	11.4.1986
Adam Smith	511-472-13-14	2.2.1967

MASKED DATA

Name	Phone	Birth Date
John Doe	511-111-11-11	1.2.1987
Adam Smith	511-123-45-67	10.11.1966

Data Access Manager - Benefits

- All queries are logged indisputably as searchable and indexed records
- Enforces role based data access security policies centrally and silently
- No performance degradation impact on target databases
- Users continue to use their own native client apps seamlessly
- Discovers sensitive data at data sources
- Masks data on the fly without changing the source data
- Supports wide range of databases and secure file transfer servers

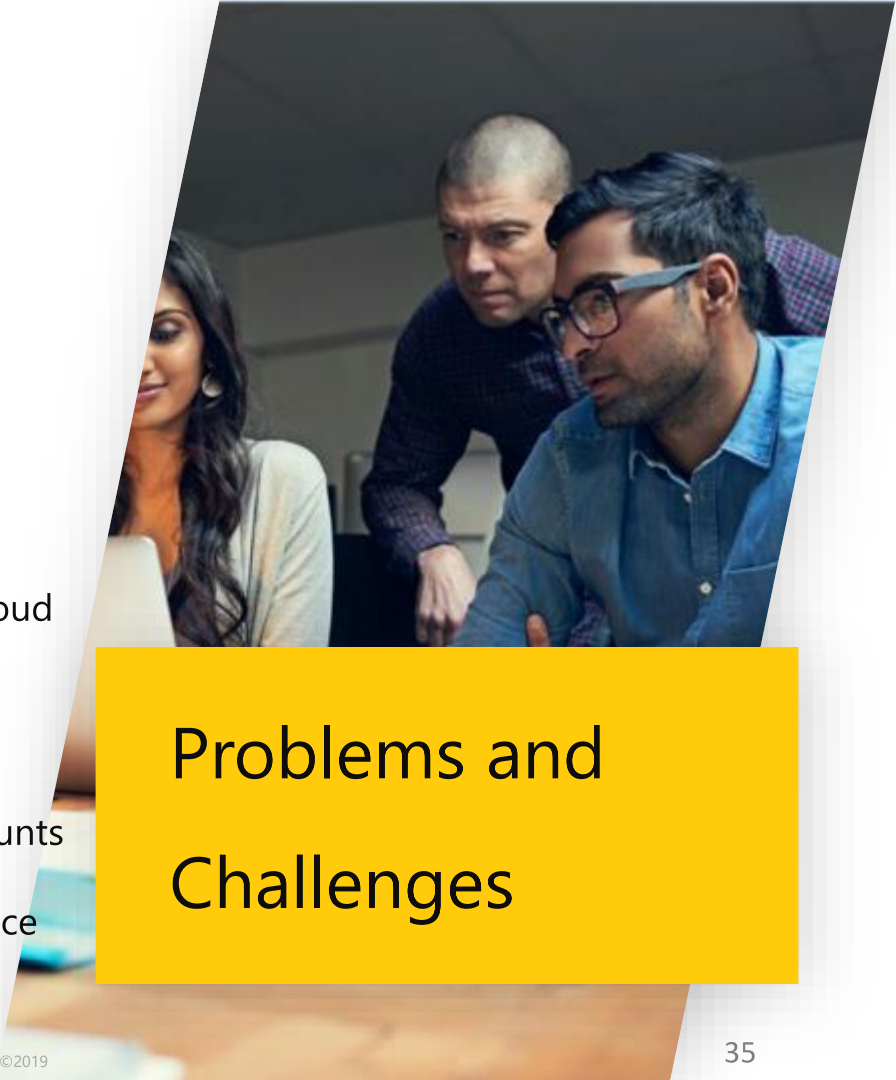


Cloud PAM

PAM services in the Cloud with zero-touch automated instance onboarding

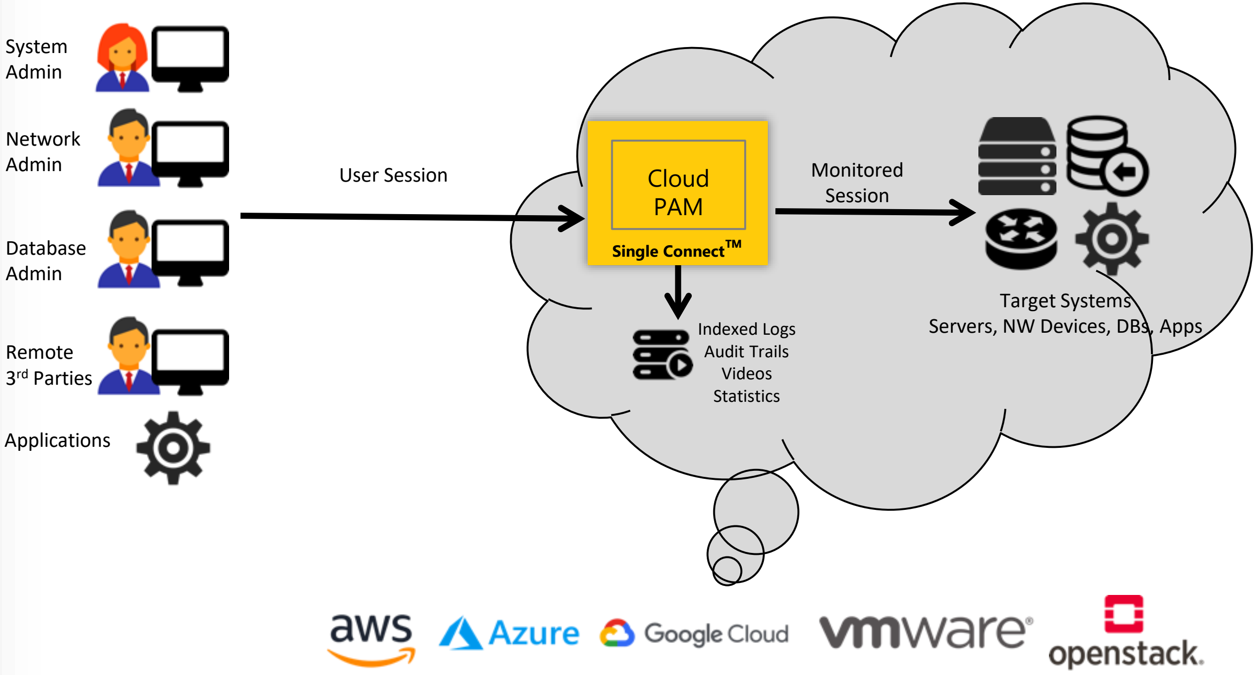
Cloud PAM

- Potential risk of malicious access from anywhere around the world, especially for public cloud platforms
- Need for extremely fast scale out and scale in. Hundreds of instances in minutes
- Various public and private cloud platforms
- Lack of central access control point for critical cloud systems
- Granting users more privileges than they need
- No or minimal accountability for privileged accounts
- Lack of data and reports for regulatory compliance and audits



Problems and Challenges

Cloud PAM Overview



Single Connect Cloud PAM Manager secures access, controls configuration changes, and records all privileged activities in public and private cloud platforms.

Cloud PAM Manager supports extremely fast scale out and scale in scenarios by auto discovering and onboarding virtual instances within minutes

All Single Connect modules and features are available to use in cloud platforms.

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- VMWare
- Openstack

Cloud PAM Manager Benefits

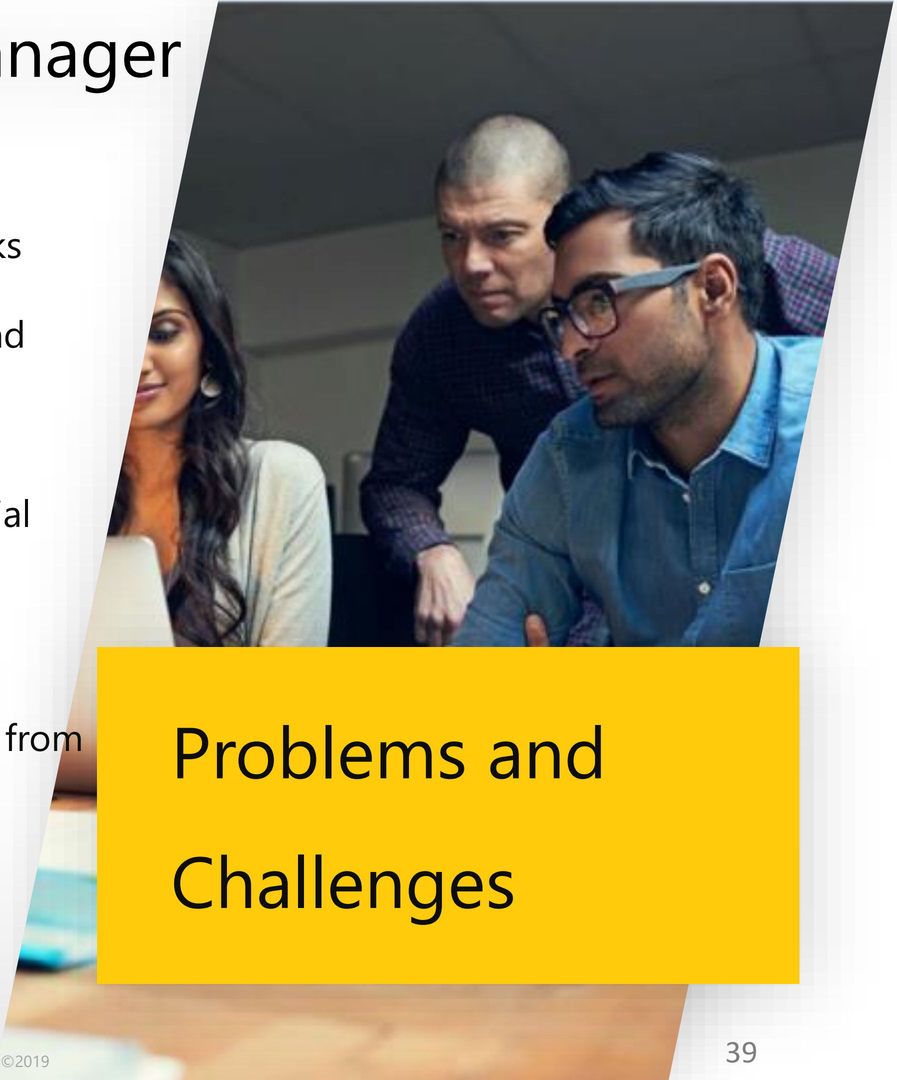
- Isolates critical target systems in cloud platforms and secures access
- Support for wide range of cloud platforms (AWS, Microsoft Azure, Google Cloud, VMWare, Openstack)
- Auto discovers/onboards virtual instances and minimizes administration tasks
- Unified visibility with searchable command / keystroke logs and replayable video recordings
- Enforces role based data access security policies centrally and silently
- Addresses regulatory requirements for privileged sessions

Privileged Task Automation Manager

Task Automation Suite for staff augmentation and granular access control

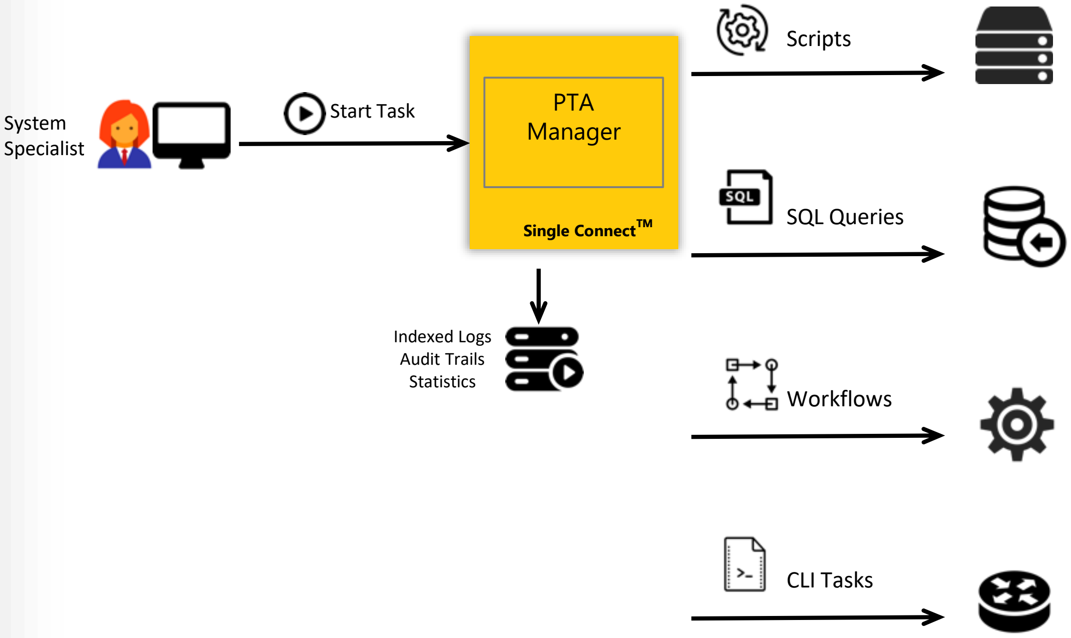
Privileged Task Automation Manager

- Time consuming repetitive and routine daily tasks
- Coordinating various departments for end-to-end configuration of a service on multiple systems
- Postponing configuration change tasks to be performed at non-business hours due to potential outage concerns
- High cost night shifts and maintenance tasks
- Lack of skilled staff to configure various systems from different vendors
- Lack of business process visibility



Problems and Challenges

Privileged Task Automation Manager Overview



Single Connect Privileged Task Automation Manager simplifies and automates daily routine tasks

Privileged Task Automation Manager provides a smart programmable interface that supports pre-check, execute, post-check and roll-back steps

Supported Interfaces

- Network Elements
- Windows Servers
- Linux Servers
- Databases
- Appliances
- REST APIs

Privileged Task Automation Manager Benefits

- Automates repetitive and routine tasks
- Enables error-free configuration changes and eliminates potential service outages
- Delegates tasks to users instead of delegating privileges
- Reduces operational costs and improves operational efficiency
- Centralized visibility of business processes and workflows
- Improves incident management process and reduces down-time
- Adapters for supporting SSH, Telnet, SNMP, XML, Netconf, JDBC, Restful API protocols
- Schedule tasks to run one-time or repetitive

Single Connect™

Protect What You Connect™

Thank You